Charles Darwin University

Final Examination

Family Name						
Given Name/s						
Student Number						
Teaching Period	Semester 2, 2018					

PRT572 – Communications and Network Security Engineering	DURATION	
	Reading Time:	10 minutes
	Writing Time:	180 minutes

INSTRUCTIONS TO CANDIDATES

Section A: Long Answer – Case Study	Marks: 10	Time allocated: 40 minutes
Section B: Short Answer. Answer any 8.	Marks: 40	Time allocated: 140 minutes

EXAM CONDITIONS

You may begin writing from the commencement of the examination session. The reading time indicated above is provided as a guide only.

This is a RESTRICTED OPEN BOOK examination

No calculators are permitted

One A4 sheet of handwritten double-sided notes permitted

No dictionaries are permitted

ADDITIONAL AUTHORISED MATERIALS	EXAMINATION MATERIALS TO BE SUPPLIED
No additional printed material is permitted	1 x 20 Page Book

THIS EXAMINATION IS PRINTED DOUBLE-SIDED.

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK.

Section A
Long Answer – Case Study
Total No of Marks for this Section: 10

This section should be answered on the Answer Sheet provided. Please ensure that your name and student number have been written on the Answer sheet and placed in the completed Answer Booklet.

Marks for each question are indicated. Suggested time allocation for Section A: 40 mins

---

Question 1

On one assessment, XYZ Security found, a global gas and oil company was communicating with remote well installations using radio communications. Internal access to the company's network could be gained by simply driving into a remote area of the wilderness, opening an unlocked utility box, and plugging a laptop into the network port readily available there. This gave the test team direct access to the SCADA and internal network of the company. Once on an internal network, attacks become much easier since internal network components are almost always less secure than the external boundary.

Based on the above scenario, answer the following questions:

1. Critically analyse the best security strategy that needs to implement to block any access.

(Marks: 2.5)

2. In your opinion, what is the biggest mistake company had made.

(Marks: 2.5)

Question 2

When presenting a talk to a group of business leaders, are you more likely to use the White Hat / Black Hat model or the Hacker profiles model to explain the dangers posed by hackers. If the business leaders are CIOs, what would be your decision? Write a short essay, explaining your answers.

(Marks: 5)

Section B
Short Answers – Answer Any Eight (8) questions only
Total No of Marks for this Section: 40

This section should be answered on the Answer Sheet provided. Please ensure that your name and student number have been written on the Answer sheet and placed in the completed Answer Booklet.

Marks for each question are indicated. Suggested time allocation for Section B: 140 mins

---

Question 1

Social engineering is an effective way to discover user passwords. Critically analyse the ways in which social engineers would gather the passwords.

(Marks: 5)

Question 2

Some security experts scan various companies' networks and then send emails informing them of their shortcomings and offering to fix those for a fee. Critically analyse whether is it an ethical marketing technique?

(Marks: 5)

Question 3

Critically analyse how Microsoft stores the user's password in MS-Windows machines

(Marks: 5)

Question 4

A friend of you is showing a vulnerably report of his company confidential and asking for suggestions to improve the security posture. What would be your stand and recommendations?

(Marks: 5)

Question 5

Critically analyse the difference between session hijacking and IP spoofing with examples.

(Marks: 5)

Question 6

Firewalls play a major role in securing the network devices. Critically analyse the limitations of firewall and list down the places where it cannot be applied.

(Marks: 5)

Question 7

Propose few strategies to mitigate the vulnerabilities in applications build by .NET framework.

(Marks: 5)

Question 8

Critically analyse the Kernel vulnerability in Unix/Linux operating systems

(Marks: 5)

Question 9

Critically analyse the phases of Incident handling with the help of a flowchart.

(Marks: 5)

Question 10

You have been hired to evaluate the security posture of a critical application and you found Buffer overflow vulnerability in the application. What would be your recommendations to avoid the vulnerability?

(Marks: 5)

!End!